REMARKS

The Examiner has rejected Claims 1, 2, 4-14, 16-26 and 28-42 under 35 U.S.C. 103(a) as being unpatentable over Nikander et al. (U.S. Patent No. 6,253,321) in view of Gitlin (U.S. Patent No. 6,757,841). Applicant respectfully disagrees with such rejection, especially in view of the amendments made to each of the independent claims.

With respect to the independent claims, the Examiner has relied on Col. 3, lines 9-65 in Gitlin to make a prior art showing of applicant's claimed "masking the portion of outgoing network data to impersonate a different operating system in accordance with a security policy if the network is an untrusted network; wherein masking the portion comprises: replacing the portion of outgoing network data with data characteristic of the different operating system" (see this or similar, but not identical language in each of the independent claims).

Applicant respectfully asserts that such excerpt from Gitlin simply discloses that "[d]uplicate data may...be written and stored in both the first location 14 and a second location 16" (see Col. 3, lines 16-18). In addition, "the first location 14 stores a first operating system and the second location 16 stores a second operating system...[such that] the mirror 30 operates to provide duplicate operating systems" (see Col. 3, lines 59-62). Thus, "since there is duplicate data, if there is problem with one of the locations, data may be read from the other location without any slowdown or failure to the system 10" (see Col. 3, lines 56-58).

Applicant respectfully asserts that simply duplicating data and/or operating systems at two storage locations does not meet applicant's specific claim language. In particular, applicant claims "masking the portion of outgoing network data" (emphasis added), and not duplicating such data. Furthermore, such masking, as claimed by applicant, is utilized "to impersonate a different operating system" (emphasis added), whereas Gitlin merely teaches duplicating (i.e. copying) the same. Still yet, nowhere in Gitlin is there even any suggestion of masking data "in accordance with a security policy

if the network is an untrusted network," as specifically claimed by applicant (emphasis added).

In addition, applicant notes that such duplication of data and/or an operating systems at two locations, as in Gitlin, also fails to meet applicant's claimed "replacing the portion of outgoing network data with data characteristic of the different operating system." Clearly, duplicating data/operating systems, as in Gitlin, does not meet any sort of replacing data for impersonating a different operating system, in the specific context claimed by applicant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has included the following claim language in each of the independent claims:

> "replacing the portion of outgoing network data with data characteristic of the different operating system to prevent identification of the operating system by impersonating the different operating system, for misleading attackers into

attempting attacks that are unworkable on the operating system" (see this or similar, but not identical language in each of the independent claims).

Applicant respectfully asserts that such claim language further distinguishes Gitlin since only applicant claims "replacing the...data... to prevent identification of the operating system by impersonating the different operating system, for misleading attackers into attempting attacks that are unworkable on the operating system" (emphasis added). Again, applicant emphasizes that Gitlin merely teaches duplicating data/operating systems at two locations, so that the data may be backed up if there is a problem at one of the locations (see Col. 3, lines 56-58), and not "replacing the...data...to prevent identification of the operating system, for misleading attackers," in the specific manner claimed by applicant.

Thus, a notice of allowance or a proper prior art showing of all of such claim limitations, in combination with the remaining claim elements, is respectfully requested. Applicant further notes that the prior art is also deficient with respect to the dependent claims.

For example, with respect to dependent Claim 4 et al., the Examiner has relied on the following excerpt from Nikander to make a prior art showing of applicant's claimed "wherein the security policy identifies the portion of outgoing network data and specifies an action to take to mask the portion of outgoing network data."

> "The policy manager may also process a received non-regular packet by itself as an alternative to compiling new filter code and communicating it to the IPSEC engine. The designer of the policy manager may decide, what kind of non-regular packets are worth compiling new filter code and what kind of packets are most advantageously processed in the policy manager. Additionally the policy manager may process a received non-regular packet by itself and compile new filter code and communicate it to the IPSEC engine for the processing of further similar packets. The last alternative is especially applicable when the received packet is a key management packet." (Col. 8, lines 1-12-emphasis added)

Applicant respectfully asserts that Nikander simply discloses a policy manager that "may also process a received non-regular packet by itself as an alternative to compiling new filter code" (see emphasized excerpt above). Such teachings clearly do not meet applicant's claimed "security policy [that] identifies the portion of outgoing network data and specifies an action to take to mask the portion of outgoing network data." Allowing a policy manager to "process" or "compile new filter code" for a non-regular packet does not meet a "security policy" that "specifies an action to take to mask the portion of outgoing data," as claimed by applicant, since there is no mention of any type of masking, etc. in Nikander (emphasis added).

With respect to dependent Claim 5 et al., the Examiner has relied on the same excerpts from Gitlin and Nikander (cited above in part) as those with regard to each of the independent claims to make a prior art showing of applicant's claimed "wherein the security policy further specifies replacement data for the portion of outgoing network data, the replacement data characteristic of the different operating system."

Applicant again respectfully asserts that duplicating data and/or operating systems at two locations (see Gitlin Col. 3, lines 9-65) in no way meets applicant's claimed "security policy" that "specifies replacement data...the replacement data characteristic of the different operating system." Simply nowhere in Gitlin or Nikander is there any mention of "replacement data," as claimed by applicant.

With respect to dependent Claim 10, the Examiner has relied on the following excerpt from Nikander to make a prior art showing of applicant's claimed "intercepting a portion of incoming network data; and sending a false response to the portion of incoming network data to impersonate the different operating system in accordance with the security policy if the network is an untrusted network."

> "A simple preferable embodiment of a method according to the invention is summarized as a flowchart in FIG. 5. Blocks 501 and 502 correspond to the operation of the packet interceptor 303 in FIG. 3, i.e. letting only IP packets reach the IPSEC engine. Blocks 503 to 507 describe operations that take place in the IPSEC engine. In block 503 the IPSEC engine applies the filter

> code it has previously stored. Applying the filter code in block 503 may include performing transformations on the packet, but this is not required by the invention. During the application of the filter code, the validity of the information stored in the IPSEC engine is also checked in block 503 for possible security association lifetime expirations or other invalidities. If the packet is a regular packet, the IPSEC engine knows whether it should drop the packet according to block 504 or accept it according to block 505; an accepted packet is output according to block 506. If the application of the filter code involved performing a transformation or otherwise processing the packet, block 506 corresponds to outputting the processed packet. If the answer in block 505 was no, the packet is non regular and it must be transferred according to block 507 to the policy manager for examination and policy rule determination according to block 508. The resulting new policy decisions are stored into the IPSEC engine at block 509 in the form of compiled filter code and the operation continues from block 503: the packet that caused the visit to blocks 508 and 509 has now become a regular one because the newly stored compiled filter code contains information about how the packet should be treated." (Col. 7, lines 39-67-emphasis added)

Applicant respectfully asserts that the above excerpt and the entire Nikander reference fail to disclose "sending a false response to the portion of incoming network data to impersonate the different operating system in accordance with the security policy if the network is an untrusted network" (emphasis added). The above excerpt merely teaches either "the accepted packet is output," "outputting the processed packed," or the packet is "transferred...to the policy manager for examination and policy rule determination" (see emphasized excerpt above), which completely fails to even suggest "sending a false response," as claimed by applicant.

A notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claim 43 below, which are added for full consideration:

"wherein the action includes discarding the portion of outgoing network data" (see Claim 43).

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P350/01.022.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100